

**Information Technology
Management Letter for the
Federal Emergency
Management Agency
Component of the FY 2015
Department of Homeland
Security Financial Statement
Audit**





DHS OIG HIGHLIGHTS

Information Technology Management Letter for the Federal Emergency Management Agency Component of the FY 2015 Department of Homeland Security Financial Statement Audit

March 8, 2016

Why We Did This

Each year, our independent auditors identify component-level information technology (IT) control deficiencies as part of the DHS consolidated financial statement audit. This letter provides details that were not included in the fiscal year (FY) 2015 DHS Agency Financial Report.

What We Recommend

We recommend that FEMA, in coordination with the DHS Chief Information Officer and Chief Financial Officer, make improvements to its financial management systems and associated information technology security program.

For Further Information:

Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

We contracted with the independent public accounting firm KPMG, LLP to perform the audit of the consolidated financial statements of the Department of Homeland Security for the year ended September 30, 2015. KPMG, LLP evaluated selected general IT controls and business process application controls at the Federal Emergency Management Agency (FEMA). KPMG, LLP determined that FEMA took corrective actions to address certain prior-year IT control deficiencies. For example, FEMA made improvements by designing and consistently implementing certain account management and configuration management controls.

However, KPMG, LLP continued to identify general IT control deficiencies related to security management, access controls, segregation of duties, configuration management, and contingency planning for FEMA's core financial and feeder systems. Collectively, these deficiencies limited FEMA's ability to ensure that critical financial and operational data were maintained in such a manner as to ensure their confidentiality, integrity, and availability.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

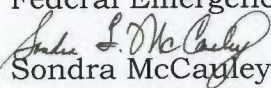
Washington, DC 20528 / www.oig.dhs.gov

March 8, 2016

MEMORANDUM FOR: Adrian Gardner
Chief Information Officer
Federal Emergency Management Agency

Thomas Lowry
Chief Financial Officer
Federal Emergency Management Agency

FROM:


Sondra McCauley
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Information Technology Management Letter for the
Federal Emergency Management Agency Component of
the FY 2015 Department of Homeland Security
Financial Statement Audit*

Attached for your information is our final report, *Information Technology Management Letter for the Federal Emergency Management Agency Component of the FY 2015 Department of Homeland Security Financial Statement Audit*. This report contains observations and recommendations related to information technology internal control deficiencies. The observations did not meet the criteria to be reported in the *Independent Auditors' Report on DHS' FY 2015 Financial Statements and Internal Control over Financial Reporting*, dated November 13, 2015, which was included in the FY 2015 DHS Agency Financial Report.

The independent public accounting firm KPMG, LLP conducted the audit of DHS' FY 2015 financial statements and is responsible for the attached information technology management letter and the conclusions expressed in it. We do not express opinions on DHS' financial statements or internal control, nor do we provide conclusions on compliance with laws and regulations. We will post the final report on our website.

Please call me with any questions, or your staff may contact Sharon Huiswoud, Director, Information Systems and Acquisitions Division, at (202) 254-5451.



KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

December 20, 2015

Office of Inspector General,
U.S. Department of Homeland Security, and
Chief Information Officer and Chief Financial Officer,
Federal Emergency Management Agency,
Washington, DC

Ladies and Gentlemen:

In planning and performing our audit of the consolidated financial statements of the U.S. Department of Homeland Security (DHS or Department), as of and for the year ended September 30, 2015 (hereinafter, referred to as the “fiscal year (FY) 2015 DHS consolidated financial statements”), in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States; and Office of Management and Budget Bulletin No. 15-02, *Audit Requirements for Federal Financial Statements*, we considered internal control over financial reporting (internal control) as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements. In conjunction with our audit of the consolidated financial statements, we also performed an audit of internal control over financial reporting in accordance with attestation standards issued by the American Institute of Certified Public Accountants.

During our audit we noted certain matters involving internal control and other operational matters at the Federal Emergency Management Agency (FEMA), a component of DHS that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies.

We identified certain internal control deficiencies at FEMA during our audit that, in aggregate and when combined with certain internal control deficiencies identified at certain other DHS Components, contributed to a material weakness in IT controls and financial system functionality at the DHS Department-wide level. Specifically, with respect to financial systems at FEMA, we noted certain matters in the general IT control areas of security management, access controls, segregation of duties, configuration management, and contingency planning. These matters are described in the *Findings and Recommendations* section of this letter.

Additionally, at the request of the DHS Office of Inspector General (OIG), we performed additional non-technical information security procedures to identify instances where FEMA personnel did not adequately comply with requirements for safeguarding sensitive material or assets from unauthorized access or disclosure. These matters are described in the *Observations Related to Non-Technical Information Security* section of this letter.



We have provided a description of key FEMA financial systems and IT infrastructure within the scope of the FY 2015 DHS financial statement audit in Appendix A, and a listing of each FEMA IT Notice of Finding and Recommendation communicated to management during our audit in Appendix B.

During our audit we noted certain matters involving financial reporting internal controls (comments not related to IT) and other operational matters at FEMA, including certain deficiencies in internal control that we consider to be significant deficiencies and material weaknesses, and communicated them in writing to management and those charged with governance in our *Independent Auditors' Report* and in a separate letter to the OIG and the FEMA Chief Financial Officer.

Our audit procedures are designed primarily to enable us to form opinions on the FY 2015 DHS consolidated financial statements and on the effectiveness of internal control over financial reporting, and therefore may not bring to light all deficiencies in policies or procedures that may exist. We aim, however, to use our knowledge of FEMA's organization gained during our work to make comments and suggestions that we hope will be useful to you.

We would be pleased to discuss these comments and recommendations with you at any time.

The purpose of this letter is solely to describe comments and recommendations intended to improve internal control or result in other operating efficiencies. Accordingly, this letter is not suitable for any other purpose.

Very truly yours,

KPMG LLP

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2015

TABLE OF CONTENTS

	Page
Objective, Scope, and Approach	2
Summary of Findings	3
Findings and Recommendations	6
Findings	6
Recommendations	7
Observations Related to Non-Technical Information Security	9

APPENDICES

Appendix	Subject	Page
A	Description of Key FEMA Financial Systems and IT Infrastructure within the Scope of the FY 2015 DHS Financial Statement Audit	11
B	FY 2015 IT Notices of Findings and Recommendations at FEMA	16

OBJECTIVE, SCOPE, AND APPROACH

Objective

We audited the consolidated financial statements of the U.S. Department of Homeland Security (DHS or Department) for the year ended September 30, 2015 (hereinafter, referred to as the “fiscal year (FY) 2015 DHS consolidated financial statements”). In connection with our audit of the FY 2015 DHS consolidated financial statements, we performed an evaluation of selected general information technology (IT) controls (GITCs), IT entity-level controls (ELCs), and IT application controls at the Federal Emergency Management Agency (FEMA), a component of DHS, to assist in planning and performing our audit engagement. At the request of the DHS Office of Inspector General (OIG), we also performed additional information security testing procedures to assess certain non-technical areas related to the protection of sensitive IT and financial information and assets.

Scope and Approach

General Information Technology Controls and IT Entity-Level Controls

The *Federal Information System Controls Audit Manual* (FISCAM), issued by the U.S. Government Accountability Office (GAO), formed the basis of our GITC and IT ELC evaluation procedures.

FISCAM was designed to inform financial statement auditors about IT controls and related audit concerns to assist them in planning their audit work and to integrate the work of auditors with other aspects of the financial statement audit. FISCAM also provides guidance to auditors when considering the scope and extent of review that generally should be performed when evaluating GITCs and the IT environment of a Federal agency. FISCAM defines the following five control categories to be essential to the effective operation of GITCs, IT ELCs and the IT environment:

1. *Security Management* – Controls that provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related security controls.
2. *Access Control* – Controls that limit or detect access to computer resources (data, programs, equipment, and facilities) and protect against unauthorized modification, loss, and disclosure.
3. *Configuration Management* – Controls that help prevent unauthorized changes to information system resources (software programs and hardware configurations) and provide reasonable assurance that systems are configured and operating securely and as intended.
4. *Segregation of Duties* – Controls that constitute policies, procedures, and an organizational structure to manage who can control key aspects of computer-related operations.
5. *Contingency Planning* – Controls that involve procedures for continuing critical operations without interruption, or with prompt resumption, when unexpected events occur.

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2015

While each of these five FISCAM categories were considered during the planning and risk assessment phase of our audit, we selected GITCs and IT ELCs for evaluation based on their relationship to the ongoing effectiveness of process-level automated controls or manual controls with one or more automated components. This includes those controls that depend on the completeness, accuracy, and integrity of information provided by the entity in support of our financial audit procedures. Consequently, FY 2015 GITC and IT ELC procedures at FEMA did not necessarily represent controls from each FISCAM category.

Business Process Application Controls

Where relevant GITCs were determined to be operating effectively, we performed testing over selected IT application controls (process-level controls that were either fully automated or manual with an automated component) on financial systems and applications to assess the financial systems' internal controls over the input, processing, and output of financial data and transactions.

FISCAM defines Business Process Application Controls as the automated and/or manual controls applied to business transaction flows and related to the completeness, accuracy, validity, and confidentiality of transactions and data during application processing. They typically cover the structure, policies, and procedures that operate at a detailed business process (cycle or transaction) level and operate over individual transactions or activities across business processes.

Financial System Functionality

In recent years, we have noted that limitations in FEMA's financial systems' functionality may be inhibiting the agency's ability to implement and maintain internal controls, including effective GITCs and IT application controls supporting financial data processing and reporting. Many key financial and feeder systems have not been substantially updated since being inherited from legacy agencies several years ago. Therefore, in FY 2015, we continued to evaluate and consider the impact of financial system functionality on internal control over financial reporting.

Non-Technical Information Security Testing

To complement our IT controls test work, we conducted limited after-hours physical security testing and social engineering at selected FEMA facilities to identify potential weaknesses in non-technical aspects of IT security. This includes those related to FEMA personnel awareness of policies, procedures, and other requirements governing the protection of sensitive IT and financial information and assets from unauthorized access or disclosure. This testing was performed in accordance with the FY 2015 DHS *Security Testing Authorization Letter (STAL)* signed by KPMG LLP, DHS OIG, and DHS management.

Appendix A provides a description of the key FEMA financial systems and IT infrastructure within the scope of the FY 2015 DHS financial statement audit.

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2015

SUMMARY OF FINDINGS

During FY 2015, we noted that FEMA took corrective action to address certain prior year IT control deficiencies. For example, FEMA made improvements over designing and consistently implementing certain account management and configuration management controls. However, we continued to identify GITC deficiencies related to controls over security management, access controls, segregation of duties, configuration management, and contingency planning for FEMA core financial and feeder systems. In many cases, new control deficiencies reflected weaknesses over new systems in scope for FY 2015 that were remediated or historically effective in other system environments.

The conditions supporting our findings collectively limited FEMA's ability to ensure that critical financial and operational data were maintained in such a manner to ensure confidentiality, integrity, and availability. In addition, certain of these deficiencies at FEMA adversely impacted the internal controls over DHS's financial reporting and its operation and we consider them to collectively contribute to a Department-wide material weakness regarding IT controls and financial system functionality for DHS, under standards established by the American Institute of Certified Public Accountants and the U.S. GAO.

Of the 18 IT Notices of Findings and Recommendations (NFRs) issued during our FY 2015 testing at FEMA, 15 were repeat findings, either partially or in whole from the prior year, and 3 were new findings. The 18 IT NFRs issued represent deficiencies and observations related to four of the five FISCAM GITC categories.

The majority of findings resulted from the lack of properly documented, fully designed and implemented, adequately detailed, and consistently implemented financial system controls to comply with the requirements of DHS Sensitive Systems Policy Directive 4300A, *Information Technology Security Program*, National Institute of Standards and Technology guidance, and FEMA policies and procedures, as applicable. The most significant weaknesses from a financial statement audit perspective continued to include:

1. Unauthorized or inadequately monitored access to, and activity within, system components for key FEMA financial applications; and
2. Configuration management controls that were not adequately designed, fully implemented, or operating effectively.

During our IT audit procedures, we also evaluated and considered the impact of financial system functionality on financial reporting. In recent years, we have noted that limitations in FEMA's financial systems' functionality may be inhibiting FEMA's ability to implement and maintain effective internal control and to effectively and efficiently process and report financial data. Many key financial and feeder systems have not been substantially updated since being inherited from legacy agencies several years ago. Many key FEMA financial systems were not compliant with Federal financial management system requirements as defined by the *Federal Financial Management Improvement Act of 1996 (FFMIA)* and Office of Management and Budget Circular Number A-123 Appendix D, *Compliance with FFMIA*.

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2015

While the recommendations made by us should be considered by FEMA, it is the ultimate responsibility of FEMA management to determine the most appropriate method(s) for addressing the deficiencies identified.

FINDINGS AND RECOMMENDATIONS

Findings

During our audit of the FY 2015 DHS consolidated financial statements, we identified the following GITC and IT ELC deficiencies at FEMA, certain of which, in the aggregate, contribute to the IT material weakness at the Department level:

Security Management

- Individuals with significant information security oversight and management responsibilities subject to role-based training were not fully identified by management, and compliance with specialized training requirements was not consistently tracked.
- Security authorization activities and supporting documentation and artifacts for core and feeder financial systems were not approved properly, updated timely, or documented accurately with respect to relevant system information.
- Plan of Actions and Milestones (POA&Ms) were non-compliant with DHS policy, including no periodic review, no planned and completed milestones, planned corrective actions that were not detailed, expected completion dates in the past where weaknesses remained open, cancellation of POA&Ms despite remediation efforts that were still in progress, and POA&Ms that were not documented for known weaknesses.

Access Controls and Segregation of Duties

- Policies and procedures for managing and monitoring FEMA personnel access to financial applications owned and operated on behalf of FEMA by third-party service organizations were not consistently or completely developed and formally documented.
- Audit logs for multiple financial system components (including the application, operating system, and database layers) did not include all required auditable events at an adequate level of detail and were not consistently reviewed by management or retained.
- Authority to approve elevated privileged access had not been fully delegated as required by FEMA policy.
- Procedures for managing access to financial applications were not documented and implemented timely, or were not sufficiently detailed to identify and describe all application roles, including elevated privileges within the systems, or controls to review and authorize access to such privileges.
- Strong password requirements were not consistently enforced on databases supporting financial applications.

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2015

Configuration Management

- Certain configuration-related deficiencies were identified on servers, workstations, and system software that were not remediated timely and tracked appropriately for remediation within management's POA&M.
- Controls to validate the completeness and integrity of changes to financial systems' production environments were not implemented.
- Automated controls to detect, log, and maintain auditable records of all implemented changes to the applications and supporting system software to ensure that movements of code into the production environments were appropriately controlled and limited to authorized changes were not implemented.

Contingency Planning

- Alternate processing sites for financial systems were not established. Consequently, testing of those systems' Contingency Plans (CPs), including restoration to an established alternate processing site, was not performed.

Recommendations

We recommend that the FEMA Office of the Chief Information Officer (OCIO) and Office of the Chief Financial Officer (OCFO), in coordination with the DHS OCIO and the DHS OCFO, make the following improvements to FEMA's financial management systems and associated IT security program (in accordance with FEMA and DHS requirements, as applicable):

Security Management

- Enhance existing policies and procedures for tracking individuals with significant security responsibilities in a central repository, and implement and ensure individuals are trained in accordance with DHS policy.
- Update security authorizations in accordance with DHS requirements.
- Document, prepare, and review POA&Ms in accordance with DHS requirements.

Access Controls and Segregation of Duties

- Develop and fully implement policies and procedures to manage FEMA personnel access, including initial authorization and ongoing recertification of access, to financial applications owned and operated on behalf of FEMA by third-party service organizations.

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2015

- Update the enterprise audit logging standard operating procedure (SOP) to ensure that systems meet the audit log events and frequency review requirements and are compliant with DHS policy.
- Properly document, approve, and execute delegation of authorization of administrator privileges from the FEMA authorizing official for financial systems, where applicable.
- Remove obsolete functions assigned to security groups and update system documentation to ensure it accurately reflects the configuration of groups and functions.
- Develop, finalize, approve and implement system documentation that will be verifiable, complete, and accurate to ensure that there is linkage between access rights assigned to end users.
- Finalize and implement policies and procedures for reviewing, approving, and recertifying user access and perform verification and validation to ensure compliance with DHS policy.
- Implement technical controls to ensure that passwords for financial databases accounts are configured in accordance with FEMA and DHS requirements. If necessary and justified by operational and business requirements, ensure that requests for exceptions from DHS password requirements clearly document all affected user and service accounts subject to deviations from standard controls and appropriate corresponding mitigating and/or compensating controls to monitor the activity of such accounts.

Configuration Management

- Ensure vulnerabilities identified are reviewed and remediated in accordance with the requirements specified in DHS and FEMA policy.
- Implement an enterprise-wide audit log solution to ensure adequate controls are in place for validating the completeness and integrity of changes deployed to production and continue manual controls until the enterprise-wide solution is fully implemented.
- Implement an enterprise-wide audit log solution to ensure adequate controls are in place for automatically monitoring and capturing changes deployed to the production environments.

Contingency Planning

- Allocate necessary resources to fully design, develop, and implement management's planned approach to identify and implement an alternate processing site, and conduct and document the results of contingency planning tests and exercises.

OBSERVATIONS RELATED TO NON-TECHNICAL INFORMATION SECURITY

To complement our IT controls test work during the FY 2015 audit, we performed additional non-technical information security procedures at FEMA. These procedures included after-hours physical security walkthroughs and social engineering to identify instances where FEMA personnel did not adequately comply with requirements for safeguarding sensitive material or assets from unauthorized access or disclosure. These procedures were performed in accordance with the FY 2015 STAL, signed by DHS OIG management, KPMG management, and DHS management on May 20, 2015, and transmitted to the DHS CIO Council on May 27, 2015.

Social Engineering

Social engineering is defined as the act of manipulating people into performing actions or divulging sensitive information. The term typically applies to trickery or deception for the purpose of gathering information or obtaining computer system access. The objective of our social engineering tests was to identify the extent to which FEMA personnel were willing to divulge network or system passwords that, if exploited, could compromise FEMA sensitive information.

To conduct this testing, we made phone calls from various FEMA locations at various times throughout the audit. Posing as FEMA technical support personnel, we attempted to solicit access credentials from FEMA users. Attempts to log into FEMA systems were not performed; however, we assumed that disclosed passwords that met the minimum password standards established by DHS policy were valid exceptions. During social engineering performed at FEMA, we attempted to call a total of 45 employees and contractors and reached 12. Of those 12 individuals with whom we spoke, one divulged passwords in violation of DHS policy.

The selection of attempted or connected calls was not statistically derived, and, therefore, the results described here should not be used to extrapolate to FEMA as a whole.

After-Hours Physical Security Walkthroughs

Multiple DHS policies, including the DHS Sensitive Systems Policy Directive 4300A, the DHS Privacy Office *Handbook for Safeguarding Sensitive Personally-Identifiable Information (PII)*, and DHS Management Directive (MD) 11042.1, *Safeguarding Sensitive but Unclassified (SBU) (FOUO) Information*, mandate the physical safeguarding of certain materials and assets that, if compromised either due to external or insider threat, could result in unauthorized access, disclosure, or exploitation of sensitive IT or financial information.

We performed procedures to determine whether FEMA personnel consistently exercised responsibilities related to safeguarding sensitive materials as defined in these policies. Specifically, we performed escorted walkthroughs of workspaces – including cubicles, offices, shared workspaces, and/or common areas (e.g., areas where printers were hosted) – at FEMA facilities that processed, maintained, and/or had access to financial data during FY 2015. We inspected workspaces to identify instances where materials

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2015

designated by DHS policy as requiring physical security from unauthorized access were left unattended. Exceptions noted were validated by designated representatives from FEMA, DHS OIG, and DHS OCIO.

During after-hours physical security walkthroughs performed at FEMA, we inspected a total of 198 workspaces. Of those, 53 were observed to have material – including, but not limited to, system passwords, information marked “FOUO” or otherwise meeting the criteria established by DHS MD 11042.1, documents containing sensitive PII, and government-issued laptops, mobile devices, or storage media – left unattended and unsecured after business hours in violation of DHS policy.

The selection of inspected areas was not statistically derived, and, therefore, the results described here should not be used to extrapolate to FEMA as a whole.

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2015

Appendix A

Description of Key FEMA Financial Systems and IT Infrastructure within the Scope of the FY 2015 DHS Financial Statement Audit

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2015

Below is a description of the significant FEMA financial management systems and supporting IT infrastructure included in the scope of the FY 2015 DHS financial statement audit.

Federal Emergency Management Agency (FEMA)

Web Integrated Financial Management Information System (WebIFMIS)

WebIFMIS is a web-based major application and the official accounting system of record for FEMA. It maintains and is the source of all financial data for both internal and external financial reporting. It is comprised of five subsystems (Funding, Cost Posting, Disbursements, Accounts Receivable, and General Ledger) that budget, record, and track all financial transactions, manage vendor accounts, and process approved payments to grantees, FEMA employees, contractors, and other vendors.

WebIFMIS contains interfaces with internal FEMA feeder systems and external service providers, including the Department of Treasury's Bureau of the Fiscal Service, the U.S. Department of Agriculture's (USDA) National Finance Center (NFC), and the Department of Health and Human Services (HHS) Grants Management System.

WebIFMIS is a commercial off-the-shelf (COTS) software package developed and maintained by Digital Systems Group, Inc., and hosted and supported by the FEMA OCFO and FEMA OCIO exclusively for internal use by the OCFO user community.

WebIFMIS is supported by an Oracle database with Linux servers. The system resides in Mt. Weather, VA.

Payment and Reporting System (PARS)

PARS is a web-based major application that includes a public-facing component that collects quarterly Standard Form (SF) 425 (Federal Financial Report) submissions and payment requests from grantees. Through daily automated scheduled jobs, grant and obligation information is updated via an interface between PARS and WebIFMIS. An internal component (OCFO) provides FEMA staff with the ability to view SF 425 submissions, examine grantee payment history reports, and add or remove holds on grantee payments.

PARS is hosted and supported by FEMA OCFO for external use by grantees and internal use by the OCFO user community.

PARS is supported by an Oracle database with HP-UX servers. The system resides in Mt. Weather, VA.

Non-Disaster Grant Management System (NDGrants)

NDGrants is a web-based major application intended to provide FEMA and its stakeholders with a system that supports the grants management lifecycle. FEMA provides state and local governments with preparedness program funding in the form of Non-Disaster Grants to enhance the capacity of state and

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2015

local emergency responders to prevent, respond to, and recover from weapons of mass destruction terrorism incidents involving chemical, biological, radiological, nuclear, and explosive devices and cyber-attacks.

NDGrants includes a public-facing component that permits external grantees and stakeholders to apply for grants, monitor the progress of grant applications and payments, and view related reports. NDGrants also has an internal component used by the FEMA Grants Program Directorate (GPD), Program Support Division (PSD), to review, approve, and process grant awards. It contains an interface with the HHS Grants.gov system to facilitate upload and integration of information submitted via SF 424 (Application for Federal Assistance).

NDGrants is hosted and supported by FEMA GPD and FEMA OCIO for external use by grantees and stakeholders and internal use by the GPD user community.

NDGrants is supported by an Oracle database with Linux servers. The system resides in Mt. Weather, VA.

Assistance to Firefighters Grants (AFG)

AFG is a web-based major application developed to assist the United States Fire Administration (USFA) division of FEMA in managing the AFG program. The primary goal of AFG is to meet the firefighting and emergency response needs of fire departments, first responders, and nonaffiliated emergency medical service organizations to obtain equipment, protective gear, emergency vehicles, training, and other resources to protect the public and emergency personnel from fire and related hazards.

AFG includes a public-facing component that permits external grantees and stakeholders to apply for grants and submit payments and reports, and an internal component used by the GPD PSD and the AFG Program Office to review, approve, and process grant awards.

AFG is hosted and supported by FEMA GPD and FEMA OCIO for external use by grantees and stakeholders and internal use by the GPD user community.

AFG is supported by an Oracle database with Linux servers. The system resides in Mt. Weather, VA.

Emergency Management Mission Integrated Environment (EMMIE)

EMMIE is a web-based major application used by FEMA program offices and user communities directly involved in the grant lifecycles associated with the Public Assistance grant program. These include Fire Management Assistance grants to provide assistance to State, Tribal, and local governments, and certain types of private nonprofit organizations so that communities can quickly respond to and recover from major disasters or emergencies declared by the President.

EMMIE includes a public-facing component that permits external grantees and stakeholders to apply for grants, and an internal component used by the different communities of interest involved in the successful

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2015

processing of a grant from solicitation to closeout and assisting with coordination between the respective program and grants management offices and the Office of Legislative Affairs. The system also contains an interface with the Environmental and Historic Preservation Management Information System (EMIS) to automate the process of reviewing and documenting FEMA-funded projects for environmental and historic preservation (EHP) compliance.

EMMIE is hosted and supported by the FEMA Public Assistance Division (PAD) and the FEMA OCIO for external use by grantees and stakeholders and internal use by the FEMA user community.

EMMIE is supported by an Oracle database with Linux servers. The system resides in Mt. Weather, VA.

Emergency Support (ES)

ES is a web-based major application that performs front-end financial management for disaster processing and controls and monitors FEMA's funds and external financial interfaces. As a module of the National Emergency Management Information System (NEMIS), ES pre-processes financial transactions, including allocation, commitment, obligation, mission assignment, and payment requests from other NEMIS modules and other external systems and serves as the primary interface to WebIFMIS. ES supports the Enterprise Coordination and Approvals Processing System (eCAPS), which provides support to initiate, track, and expedite the process of providing direct aid and technical assistance, including electronic coordination and approval of internal requisitions for services and supplies, and mission assignments, to other Federal agencies and states in response to Presidentially-declared disasters.

ES includes a public-facing component that permits access for applicants for grants or disaster assistance and other state, local, and non-governmental organization (NGO) representatives and members of the public. It also includes an internal component used by FEMA OCFO to process disaster housing payments, perform payment recoupment, and conduct other administrative tasks associated with disaster payments.

In addition to WebIFMIS and eCAPS, ES contains interfaces with other internal FEMA feeder systems, including EMMIE and AFG.

ES is hosted and supported by the FEMA OCFO and FEMA OCIO for external use by grantees and stakeholders and internal use by the OCFO user community.

ES is supported by an Oracle database with Linux servers. The system resides in Mt. Weather, VA.

Transaction Recording and Reporting Processing (TRRP)

TRRP is a mainframe-based application and a subsystem of the National Flood Insurance Program (NFIP) Information Technology System (ITS) GSS that collects, maintains, and reports on all data and activity submitted by the Write Your Own (WYO) companies and the Direct Servicing Agent (DSA) for NFIP. Additionally, TRRP creates and updates policies, claims, and community master files that are maintained on the NFIP ITS mainframe.

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2015

TRRP is hosted and supported by Computer Sciences Corporation (CSC), Inc., on behalf of the Federal Insurance & Mitigation Administration, exclusively for internal use by the NFIP user community.

TRRP is supported by a FOCUS database with an IBM z/OS mainframe. The system resides in Norwich, CT.

Payment Management System (PMS)

The PMS, commonly referred to as Smartlink, is a web-based major application hosted, developed, operated, and maintained by the HHS National Institutes of Health (NIH) Center for Information Technology (CIT) Information Systems Branch (ISB). The FEMA OCFO's Finance Center user community uses Smartlink to disburse grant funds to grantees, track and maintain grantee payment and expenditure data, and manage cash advances to recipients.

PMS is supported by an Oracle database with HP-UX servers. The system resides in Bethesda,

Web Time and Attendance (WebTA)

WebTA is a COTS web-based major application hosted by the USDA NFC and developed, operated, and maintained by the NFC IT Services Division and NFC Risk Management Staff. The FEMA Office of the Chief Component Human Capital Officer (OCCHCO) utilizes NFC and WebTA to process front-end input and certification of time and attendance entries by the FEMA user community to facilitate payroll processing.

EmpowHR

EmpowHR is a COTS web-based major application hosted by the NFC and developed, operated, and maintained by the NFC IT services division and NFC Risk Management Staff. DHS components utilize NFC and EmpowHR to initiate, authorize, and send personnel data to NFC for processing.

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
September 30, 2015

Appendix B

FY 2015 IT Notices of Findings and Recommendations at FEMA

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
 September 30, 2015

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FEMA-IT-15-01	Non-Compliance with DHS Secure Baseline Configuration Guidance for Oracle Database User Account Passwords	Access Controls		X
FEMA-IT-15-02	Inconsistent Implementation of WebIFMIS and PARS Audit Log Controls	Access Controls		X
FEMA-IT-15-03	Lack of Controls to Validate Completeness and Integrity of Changes Deployed to Production for the WebIFMIS and PARS Production Environments	Configuration Management		X
FEMA-IT-15-04	Lack of Automated Controls to Log Changes Deployed to Production for the EMMIE, the NDG, the ES, and the AFG Systems	Configuration Management		X
FEMA-IT-15-05	Insufficient Audit Log Controls for Key Financial Systems	Access Controls		X
FEMA-IT-15-06	Inconsistent Delegation of Authority and Authorization of Privileged Access for Systems Managed by OCIO IT Operations	Access Controls		X
FEMA-IT-15-07	NACS Account Management Weaknesses	Access Controls	X	
FEMA-IT-15-08	Non-Compliance with Alternative Processing Site Requirements for Key Financial Systems	Contingency Planning		X
FEMA-IT-15-09	Security Awareness Issues Identified during Social Engineering Testing at FEMA	Security Management		X
FEMA-IT-15-10	Security Awareness Issues Identified during After-Hours Physical Security Testing at FEMA	Security Management		X
FEMA-IT-15-11	Non-Compliant Security Authorization Packages for Key Financial Systems	Security Management		X

Department of Homeland Security
Information Technology Management Letter
Federal Emergency Management Agency
 September 30, 2015

FY 2015 NFR #	NFR Title	FISCAM Control Area	New Issue	Repeat Issue
FEMA-IT-15-12	Lack of Web Time and Attendance (WebTA) Account Management Policies and Procedures	Access Controls		X
FEMA-IT-15-13	Incomplete Implementation of Role-Based Training for Individuals with Significant Information Security	Security Management		X
FEMA-IT-15-14	Incomplete Documentation of Web Integrated Financial Management Information System (WebIFMIS) Application Functions	Access Controls and Segregation of Duties		X
FEMA-IT-15-15	Lack of Smartlink Account Management Policies and Procedures	Access Controls		X
FEMA-IT-15-16	Weaknesses Identified Through Vulnerability Management Procedures on Financially Significant Segments of the FEMA Enterprise Network (FEN) and End-User Computing Environment	Configuration Management		X
FEMA-IT-15-17	Non-Compliant Plan of Action and Milestone (POA&M) reporting for Key Financial Systems	Security Management	X	
FEMA-IT-15-18	Inconsistent Implementation of EmpowHR Account Management Controls	Access Controls	X	



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix E
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Under Secretary for Management
Chief Privacy Officer

Federal Emergency Management Agency

Administrator
Chief Financial Officer
Chief Information Officer
Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.



OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305